From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 06 June 2000 (06.06.00)	
International application No. PCT/GB99/03140	**Applicant's or agent's file reference** MCK/P21102GB
International filing date (day/month/year) 21 September 1999 (21.09.99)	**Priority date** (day/month/year) 21 September 1998 (21.09.98)
Applicant PERKINS, Rodney	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

12 April 2000 (12.04.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Olivia RANAIVOJAONA
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

V1

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION TO THE DESIGNATED OFFICE OF RECEIPT OF RECORD COPY

(PCT Administrative Instructions, Section 426)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as designated Office

Date of mailing (day/month/year)	**Applicant's or agent's file reference**
25 November 1999 (25.11.99)	MCK/P21102GB

The designated Office is hereby notified that the International Bureau has received the record copy of the international application identified below:

Applicant(s):

International application No.	:	PCT/GB99/03140
International filing date	:	21 September 1999 (21.09.99)
Priority date(s) claimed	:	21 September 1998 (21.09.98)
Date of receipt of the record copy by the International Bureau	:	02 November 1999 (02.11.99)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Patricia Gonzalez

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL BUREAU

To:
KINSLER, Maureen, Catherine
Kilburn & Strode
20 Red Lion Street
London WC1R 4PJ
ROYAUME-UNI

K + S Received
Date: 10 APR 2000

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

Date of mailing (day/month/year) 30 March 2000 (30.03.00)	
Applicant's or agent's file reference MCK/P21102GB	**IMPORTANT NOTICE**

International application No.	**International filing date** (day/month/year)	**Priority date** (day/month/year)
PCT/GB99/03140	21 September 1999 (21.09.99)	21 September 1998 (21.09.98)

Applicant
THE POST OFFICE et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
   AU,CN,JP,KP,KR,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   AE,AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CR,CU,CZ,DE,DK,DM,EA,EE,EP,ES,FI,GB,GD,GE,
   GH,GM,HR,HU,ID,IL,IN,IS,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MD,MG,MK,MN,MW,MX,NO,NZ,OA,
   PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW
   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
   30 March 2000 (30.03.00) under No. WO 00/18060

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, **a demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
J. Zahra

Telephone No. (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
MCK/P21102GB		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/GB99/03140	21/09/1999	21/09/1998
International Patent Classification (IPC) or national classification and IPC H04L29/06		
Applicant THE POST OFFICE et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 11 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
12/04/2000	06.12.2000
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Dechmann, J-L Telephone No. +49 89 2399 8826

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB99/03140

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:
Description, pages:

1,2,5-8,11-16	as originally filed			
3,4,4a,9,10	as received on	24/08/2000	with letter of	22/08/2000

Claims, No.:

1-8	as received on	24/08/2000	with letter of	22/08/2000

Drawings, sheets:

1/4-4/4	as received on	24/08/2000	with letter of	22/08/2000

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-8
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-8
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-8
	No:	Claims	

2. Citations and explanations
   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement

I

The following documents have been considered for the purposes of this report:

D1: EP-A-0 798 892
D2: US-A-5 557 765
D3: J. LINN: 'Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and authentication procedures' RFC1421, [Online] February 1993 (1993-02), pages 6-30, XP002132590 Retrieved from the Internet: <URL:ftp://ftp.isi.edu/in-notes/rfc1421.tx t> [retrieved on 2000-03-09]

II

The present application relates to secure data transfer involving a trusted third party (TTP).
There is a need for an electronic equivalent of the recorded and registered postal system.
It has been proposed that recorded e-mail delivery can be effected by using an encryption system by which an encrypted message is transfered to and held by a central point associated with a TTP for onward delivery to an authenticated user. The message is stored at the TTP until it is requested by the intended recipientto notification that the message is waiting. Thus the system is dependent upon the storage capacity of the TTP.

In the invention, the secure data transfer system includes sender, receiver and key facility. The sender encrypts data and splits it into parts. The key facility encrypts a part of the data and sends it to the receiver. The receiver requests for decryption of the part

encrypted by the key facility and then decrypts the entire data. The recipient is assured of the integrity of the entire data by the signature. The encrypted data can be sent to the recipient in a format that is agreed with the sender.

None of the cited documents suggest such a solution and an inventive step is therefore acknowledged (see analysis of these documents in the amended description pages 3 and 4). An inventive step is therefore acknowledged.

The requirements of Article 33(3) PCT are fulfilled for claims 1-8

VII. Certain defects in the international application

1. The reference to the "spirit" of the invention should be deleted on page 16 (PCT Guidelines C-III-4.3a and Article 6 PCT).

VIII. Certain observations on the international application

Claim 1 lacks clarity (Article 6 PCT) in that it is not understood from the formulation of claim 1 if the third party (TTP) is the same entity as the key facility or not.
Line 4 of claim 1 mentions "...**a key facility**..." whereas line 7 mentions "...means for encrypting at least one of the parts for **a third party...**". Is it the same entity or another separate entity? The use of an undefinite article suggested that it is indeed a different entity.

The description on page 8 at lines 10 to 12 however specifies that "the TTP can be referred to as a key facility", it seems therefore that the key facility and the TTP are in fact a single entity.
If it is the case, then for reason of consistency of terminology only one term should be used for the two entities (Rule 10.2 PCT) or it should be clearly specified in claim 1 that they are the same: line 7 could be amended the following way:"...**the key facility or** third party.

15

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
MCK/P21102GB		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/GB99/03140	21/09/1999	21/09/1998
International Patent Classification (IPC) or national classification and IPC H04L29/06		
Applicant THE POST OFFICE et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 11 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
12/04/2000	06.12.2000
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Dechmann, J-L Telephone No. +49 89 2399 8826

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB99/03140

I. Basis of the report

1. This report has been drawn on the basis of *(substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments (Rules 70.16 and 70.17).)*:
Description, pages:

1,2,5-8,11-16	as originally filed			
3,4,4a,9,10	as received on	24/08/2000	with letter of	22/08/2000

Claims, No.:

1-8	as received on	24/08/2000	with letter of	22/08/2000

Drawings, sheets:

1/4-4/4	as received on	24/08/2000	with letter of	22/08/2000

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-8
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-8
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-8
	No:	Claims	

2. Citations and explanations
   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement

I

The following documents have been considered for the purposes of this report:

D1: EP-A-0 798 892
D2: US-A-5 557 765
D3: J. LINN: 'Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and authentication procedures' RFC1421, [Online] February 1993 (1993-02), pages 6-30, XP002132590 Retrieved from the Internet: <URL:ftp://ftp.isi.edu/in-notes/rfc1421.tx t> [retrieved on 2000-03-09]

II

The present application relates to secure data transfer involving a trusted third party (TTP).
There is a need for an electronic equivalent of the recorded and registered postal system.
It has been proposed that recorded e-mail delivery can be effected by using an encryption system by which an encrypted message is transfered to and held by a central point associated with a TTP for onward delivery to an authenticated user. The message is stored at the TTP until it is requested by the intended recipientto notification that the message is waiting. Thus the system is dependent upon the storage capacity of the TTP.

In the invention, the secure data transfer system includes sender, receiver and key facility. The sender encrypts data and splits it into parts. The key facility encrypts a part of the data and sends it to the receiver. The receiver requests for decryption of the part

encrypted by the key facility and then decrypts the entire data. The recipient is assured of the integrity of the entire data by the signature. The encrypted data can be sent to the recipient in a format that is agreed with the sender.

None of the cited documents suggest such a solution and an inventive step is therefore acknowledged (see analysis of these documents in the amended description pages 3 and 4). An inventive step is therefore acknowledged.

The requirements of Article 33(3) PCT are fulfilled for claims 1-8

VII. Certain defects in the international application

1. The reference to the "spirit" of the invention should be deleted on page 16 (PCT Guidelines C-III-4.3a and Article 6 PCT).

VIII. Certain observations on the international application

Claim 1 lacks clarity (Article 6 PCT) in that it is not understood from the formulation of claim 1 if the third party (TTP) is the same entity as the key facility or not.
Line 4 of claim 1 mentions "...**a key facility**..." whereas line 7 mentions "...means for encrypting at least one of the parts for **a third party...**". Is it the same entity or another separate entity? The use of an undefinite article suggested that it is indeed a different entity.

The description on page 8 at lines 10 to 12 however specifies that "the TTP can be referred to as a key facility", it seems therefore that the key facility and the TTP are in fact a single entity.
If it is the case, then for reason of consistency of terminology only one term should be used for the two entities (Rule 10.2 PCT) or it should be clearly specified in claim 1 that they are the same: line 7 could be amended the following way:"...**the key facility or** third party.

Assurances as to the identity of the decrypter, i.e. the recipient, are just as necessary as those associated with the encrypter. To address this it is known to employ the services of a trusted third party (TTP) or certificate authority. The role of the TTP is to certify to either or both parties that the other is who they purport to be. Certification links a particular key with the identity of a party. Clearly, the security of the TTP is vital to its standing as an issuer of certificates.

The certificate typically includes identification data as well as identification of the certification authority and the duration for which the certificate is valid. A so-called distinguished name provides authentication of an identity linked to a specific capacity, e.g. rank in an organisational hierarchy. This can be used in addition to the certificate associated with the transacting site.

Encryption software enables users to communicate securely by encrypting files and attaching them to electronic mail (e-mail) messages. The files cannot be read by anybody other than the intended recipient of proven identity. There are many implementations of such software, for example that described in the article by J Linn title "Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and Authentication Procedures" RFC1421, [Online] February 1993 (1993-02), pages 6-30, XP002132590 Messaging". In all cases, however, the recipient has free access to the message, provided that the recipient's private key is available.

In some protocols there is provision for parties other than the sender or specified recipient to gain access to the contents of a message by encrypting a key and decrypting it in special circumstances. Two cases can be distinguished:

(1) an escrow capability by a known person or organisation; and (2) release of the key(s) of the message to persons not defined when the message is encrypted. US 5,557,765 describes an example of (1) where a message key is divided into parts which are separately encrypted to escrow agents so that Law Enforcement Agencies or authorised bodies can recover them later. In general this is done secretly and the sender is not able to detect that the message has been accessed. EP-A-0,798,892 discloses an example of (2), where the encryption process is not specific to any defined recipient. The intention is that any recipient can access the plaintext (or part of it) by means of a payment. In return for the payment the message key is released. It is not necessarily the case that the sender can find out the identities of those recipients.

There is a need for an electronic equivalent of the recorded and registered postal systems. In many instances, it is necessary for the sender of mail at least to have verification that it has been received by the authorised recipient (proof of delivery). A recorded postal letter is signed for by the recipient when it is handed over by the deliverer. A registered postal letter is tracked through the postal system and logged as having passed various points up to delivery.

In an e-mail system the verification of delivery is not necessarily assured because either the acknowledgement software of the recipient may be disabled or the recipient is posing as the intended recipient fraudulently. E-mail is not inherently secure. Thus, security of an e-mail message depends entirely upon encryption of the message and the encryption system remaining uncompromised.

It has been proposed that recorded e-mail delivery can be effected by using an

encryption system by which an encrypted message is transferred to, and held by, a central point associated with a TTP for onward delivery to an authenticated user. The message is stored at the TTP until it is requested by the intended recipient in response to notification that the message is waiting. However, it has been found that there is a practical limit on the amount of information the TTP can store. Thus, the system is dependent upon the storage capacity of the TTP. Furthermore, not only the encryption system but the message itself has to conform to the TTP's reception/transmission system both in terms of format and transmission medium.

According to the present invention there is provided a data transfer system as specified in claim 1. Some preferred features are defined in the dependent claims.

The data transfer transmission in which the invention is embodied comprises a sender facility; a receiver facility and a key facility; the sender facility having means for encrypting data for the intended recipient, means for splitting the data into encrypted parts such that no part is decrypted on its own, means for encrypting at least one of the parts for a third party to produce a further encrypted part, means for combining the further encrypted part and the remaining encrypted part to produce a data block and means for sending the data block, the receiver facility having means for receiving the data block, means for requesting decryption of the further encrypted part by the key facility which has means for decrypting the further encrypted part and means for sending it to the receiver facility and the receiver facility also having means for

PKCS#7 mode. The Entrust security system has various architecture components. The security is based on a choice of symmetric key algorithm, including the Data Encryption Standard (DES), Triple DES and CAST; asymmetric or public key algorithms, such a RSA, DSA and DIFFIE HELLMAN; and hashing algorithms such as SHA-1, MD2 and MD5. These are only examples of key systems. Other key systems will be known to the skilled person which could be used to equal effect. The receiver and TTP sites are similarly provided with Entrust System components configured to receive and decrypt data sent by the sender as described below.

Referring to Figure 4a, at the sender site 10 the plain text message P/T is both encrypted with the public key for the recipient K_R or a group of recipients and signed by the PEM method using the sender's private key K_S. The 'header' part of the message is split off, i.e. in the standard PEM format that part from ".....BEGIN PRIVACY-ENHANCED MESSAGE....." to the terminating empty line. This is referred to as the "inner header" 22. The remainder is the "encrypted text" 20.

Referring to Figure 4b), still at the sender site 10, the inner header 22 is further encrypted and signed by the PEM method using the public key K_{TTP} of the third party only. This produces an "encrypted header" 24 and an "outer header" 26. The encrypted text 20, encrypted inner header 24 and outer header 26 are combined and digitally signed. The Message Integrity Check (MIC) field of the Outer Header 26 is a convenient unique identifier as it is a hash of the inner header 22 which, in turn, contains a hash of the plaintext; so the outer header MIC is dependent on the contents of the plaintext. Also, the inner header varies even when the same plaintext is used as the symmetric key is

chosen at random on each occasion.

The encrypted text 20, encrypted inner header 24, the outer header 26 and signature are sent as a multi-purpose internet mail extension (MIME) within an e-mail message to form a message package. The unencrypted body of the message itself is an explanation of the sent data and instructions to the recipient on how to obtain software to decrypt the MIME inclusion.

The sender (and recipient) software for preparing the encrypted data comprises Microsoft Exchange or Outlook management software as well as the new plug-in interface. The preparation of the message is Windows-based, providing a tool bar button to click on if the service is required for encrypting e-mail transmission.

This embodiment of the invention is a form of e-mail recorded delivery. Thus, the prepared secure message is sent by the SMTP connection to the receiver site directly. At the same time an alerting message may be sent from the sender site to the TTP. Upon receipt of the e-mail message package the recipient is presented with the open e-mail message containing the instructions, the cipher text, the encrypted header, the outer header intended for the TTP. The recipient's software extracts the inner and outer headers, signs them as one block using PEM or PKCS#7 and transmits them to the TTP using TCP/IP. Thus, the receiver site is instructed by the open e-mail message to send at least the encrypted header 24 and the outer header 26 to the TTP, as indicated in Figure 4c, as a request for decryption of the encrypted header.

At the TTP the signature is checked. This process reveals the identity of the

CLAIMS:

1. A data transfer system comprising: a sender facility (10); a receiver facility (12) and a key facility (14); the sender facility (10) having means for encrypting data for the intended recipient, means for splitting the data into encrypted parts such that no part is decryptable on its own, means for encrypting at least one of the parts for a third party to produce a further encrypted part, means for combining the further encrypted part and the remaining encrypted part to produce a data block and means for sending the data block, the receiver facility (12) having means for receiving the data block, means for requesting decryption of the further encrypted part by the key facility (14) which has means for decrypting the further encrypted part and means for sending it to the receiver facility (12) and the receiver facility (12) also having means for decrypting the encrypted part and the decrypted further encrypted part provided by the key facility (14).

2. A system as claimed in claim 1 in which the sender facility (10) includes means for signing the data block.

3. A system as claimed in claim 1 or 2 in which the means for sending at the sender facility (10) are arranged to send the data block to the key facility (14) and the key facility (14) includes means for receiving the data block and forwarding the said block to the receiver facility (12).

4. A system as claimed in claim 3 in which the key facility (14) further includes means for logging receipt of the data block.

5. A system as claimed in claim 1 or 2 in which the means for sending at the sender facility (10) are arranged to send the data block to the receiver facility (12) and the receiver facility (12) includes means for receiving the data block.

6. A system as claimed in claim 5 in which the key facility (14) further includes means for logging receipt of the further encrypted part.

7. A system as claimed in any of claims 1 to 6 in which the key facility (14) includes means for logging receipt of the request for decryption of the further encrypted part as proof of delivery of the block to the receiver facility (12).

8. A system as claimed in claim 7 in which the sender facility (10) includes means for requesting proof of delivery information from the key facility (14).

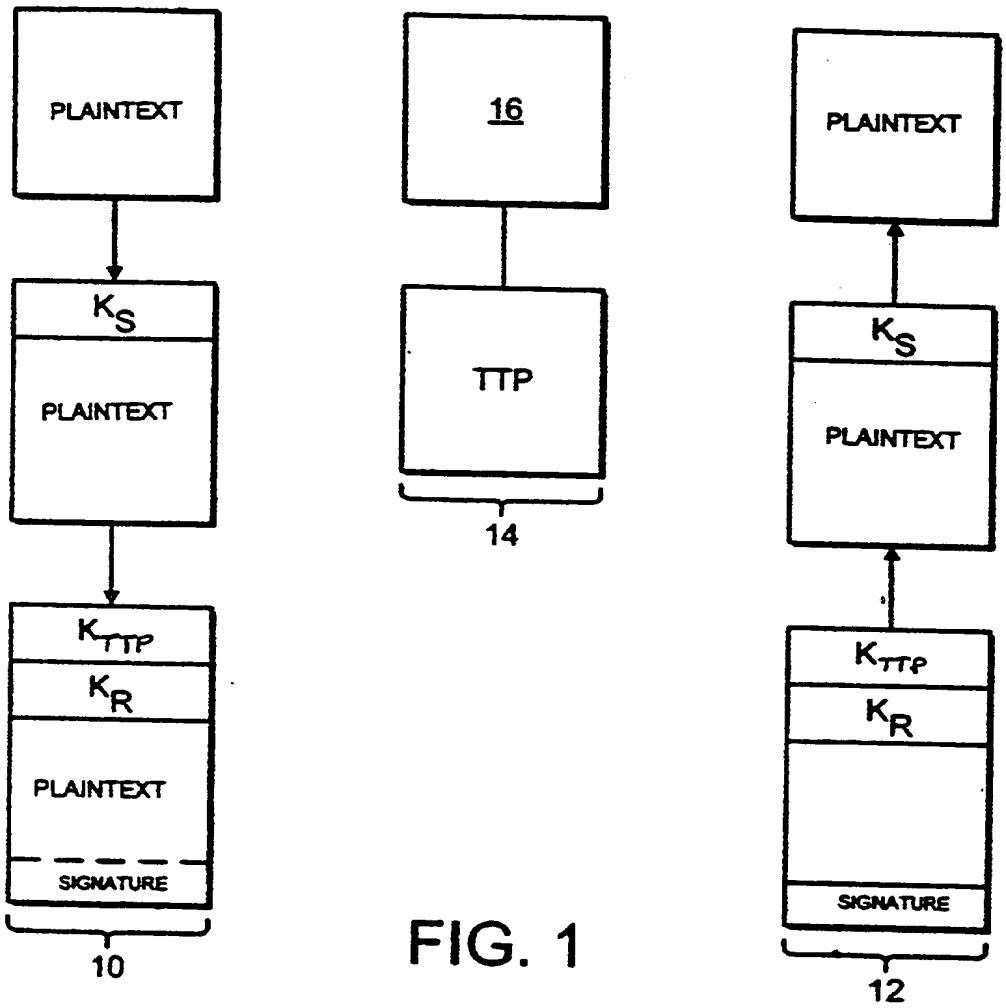
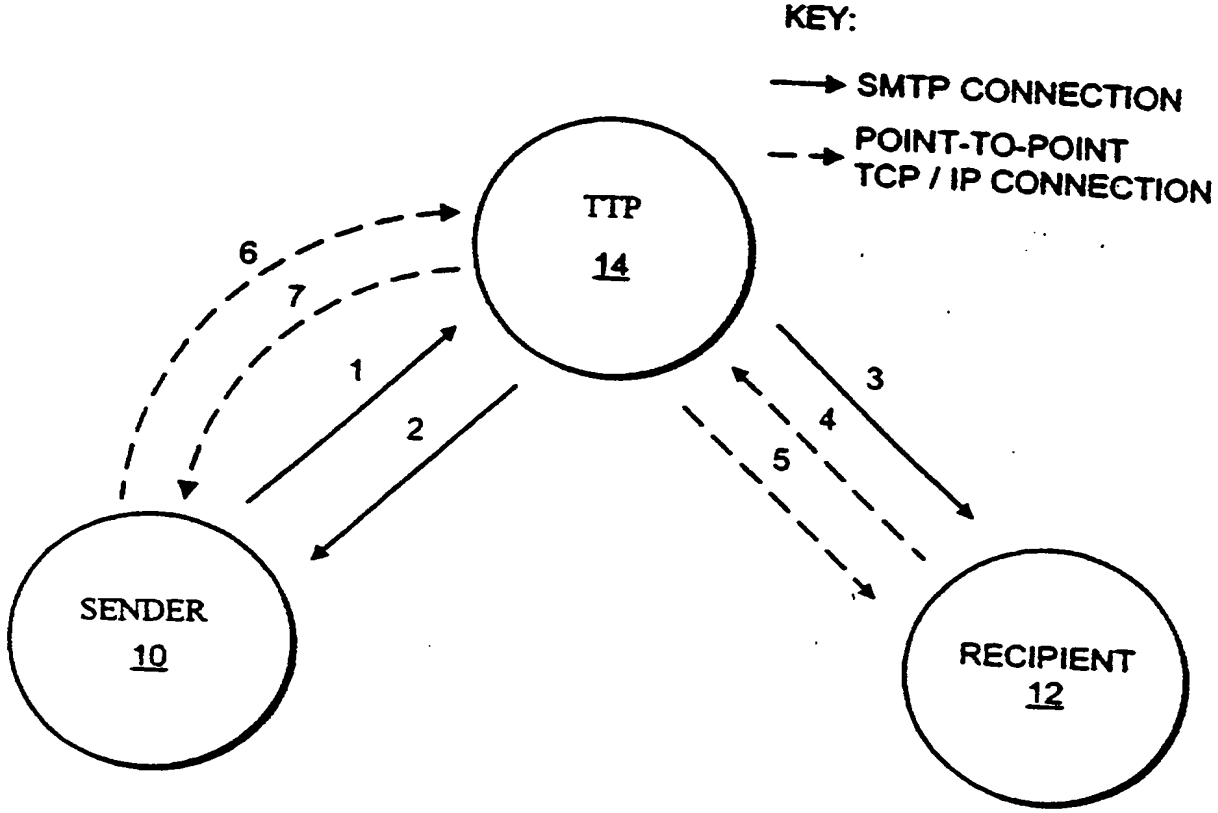

PLAINTEXT
K_S
PLAINTEXT
K_{TTP}
K_R
PLAINTEXT
SIGNATURE
10
16
TTP
14
PLAINTEXT
K_S
PLAINTEXT
K_{TTP}
K_R
SIGNATURE
12

FIG. 1

FIG. 2

SECURE COURIER WITH POST MARKING

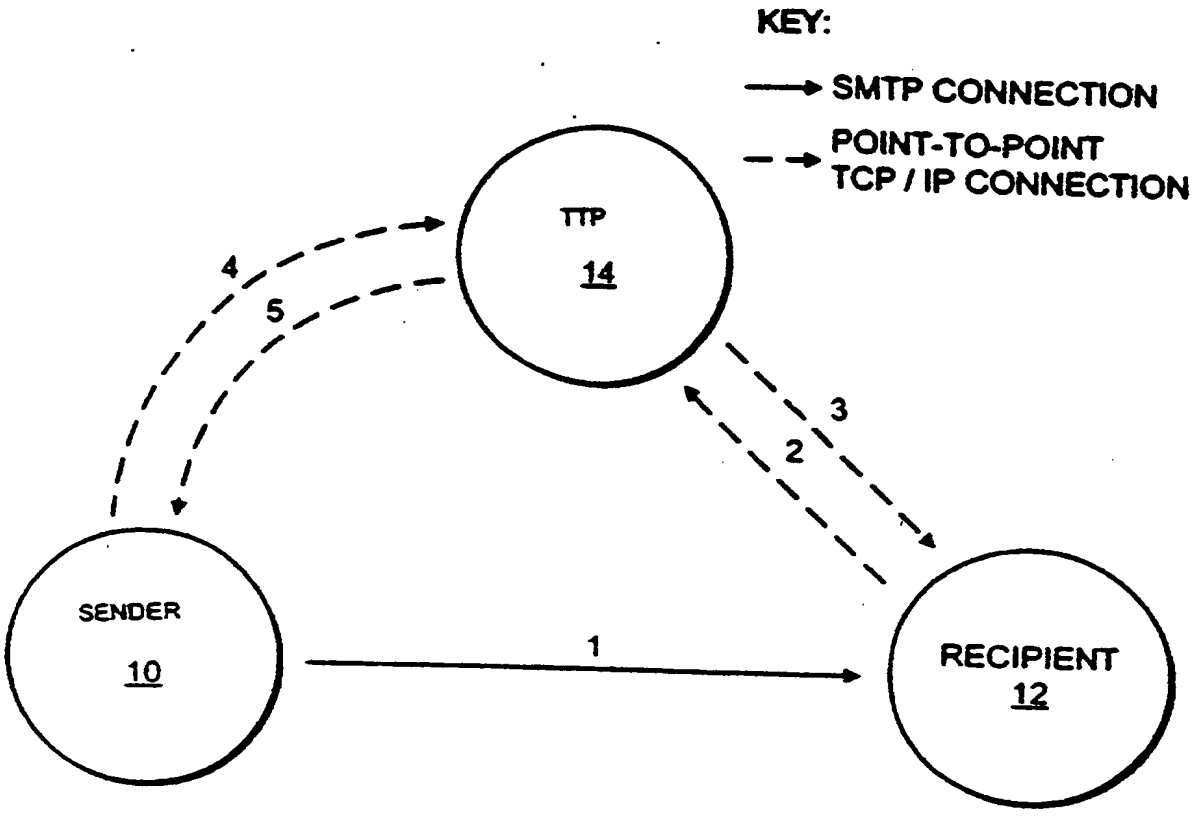


1. MESSAGE SENT FROM SENDER TO TTP
2: TTP RETURNS PROOF-OF-SUBMISSION
3: TTP DELIVERS MESSAGE
4: RECIPIENT REQUESTS THE KEY TO DECIPHER THE MESSAGE
5: TTP LOGS THE REQUEST AND RETURNS THE KEY
6: SENDER QUERIES THE STATUS OF THE MESSAGE
7: TTP RETURNS RESPONSE TO THE SENDERS' QUERY

- TTP = Trusted Third Party

FIG. 3

SECURE COURIER WITHOUT POST MARKING



1. MESSAGE SENT FROM SENDER TO RECIPIENT
2: RECIPIENT REQUESTS THE KEY TO DECIPHER THE MESSAGE
3: TTP LOGS THE REQUEST AND RETURNS THE KEY
4: SENDER QUERIES THE STATUS OF THE MESSAGE
5: TTP RETURNS RESPONSE TO THE SENDER'S QUERY

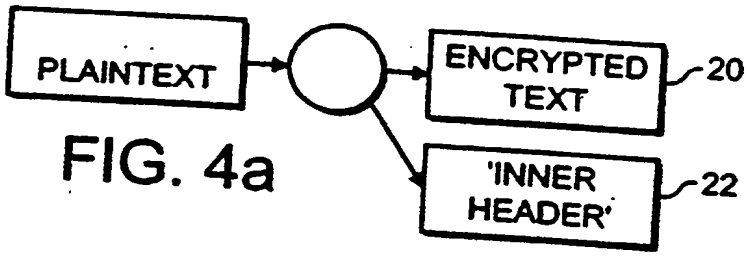


FIG. 4a

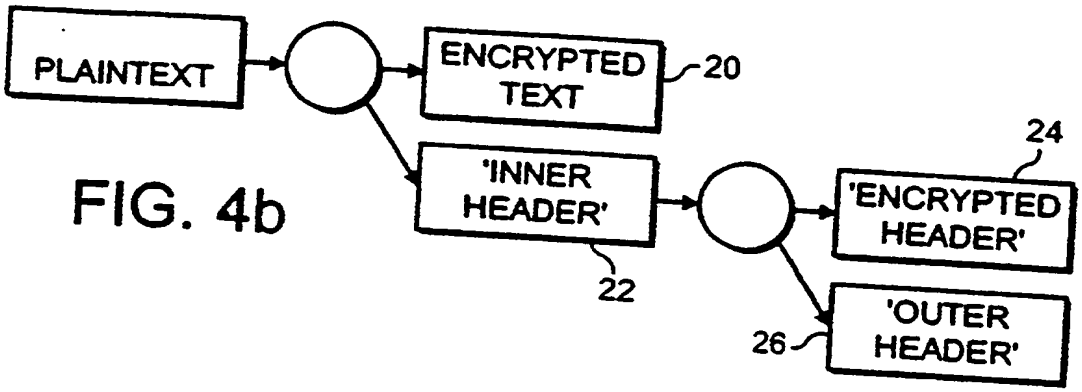


FIG. 4b

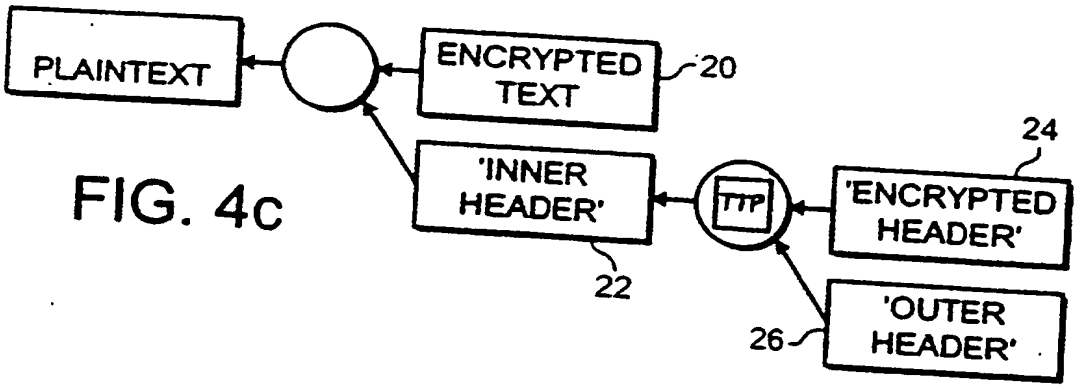


FIG. 4c

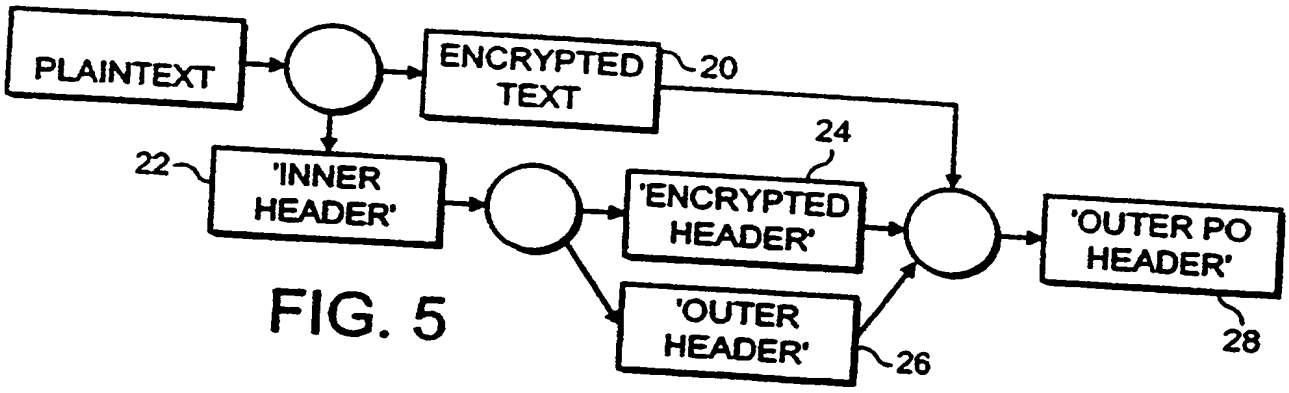


FIG. 5